RMS RedMAXEMS
User Manual

May 5, 2010

Version: 2.2.1

Part Number 70-00066-22-01

Disclaimer:

The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable; however, they are presented without express or implied warranty. Additionally, Redline **makes no representations or warranties, either expressed or implied, regarding the contents of this document.**

Redline Communications Inc. **shall not be liable for any misuse regarding this product.**

The information in this document is subject to change without notice.

Safety Notice:

The RMS **product is designed to monitor and configure** RedACCESS**,** RedCONNEX **and** RedMAX **fixed wireless broadband equipment. Operators should read the User's Manual and Installation Guide for** RedMAX **wireless products described in this manual to understand and follow all operating and safety instructions before using the** RMS**. Keep all product information for future reference.**

Confidential and Proprietary Information:

This document constitutes confidential and proprietary information of Redline Communications Inc.**. The contents of this document may be accessed and/or used solely by a licensee of** Redline Communications Inc. **software product(s) and solely in connection with the licensee's authorized use of such product(s), or as otherwise expressly permitted by** Redline Communications Inc. **in writing. All other uses are prohibited. This document may not in any event be disclosed to any third party without the prior written authorization of** Redline Communications Inc.

Trademark Information:

Redline Management Suite**™,** Redline®**,** RMS**™,** RedACCESS**™,** RedCONNEX**™ and** RedMAX**™ are trademarks of** Redline Communications Inc. **All other brands and product names identified in this publication are trademarks or registered trademarks of their respective companies or organizations.**

Copyright © 2010, Redline Communications Inc.

All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems for any purpose without the express written permission of Redline Communications Inc.

Table of Contents

CHAPTER 1 **About This Guide**

- Overview 1-1
- About This Document 1-1
- Document Conventions 1-2
- System Behavior 1-3
  - RMS Operations 1-3
  - Network Elements 1-3
  - Web Client 1-4

CHAPTER 2 **RMS User Interface**

- Overview 2-1
- Logging into the RMS Client 2-3
  - User Account Management 2-5
  - Your Browser's Pop-up Blocker 2-5
- Working with the RMS User Interface 2-5
  - Main Menu 2-5
    - Fault Menu 2-6
    - Config Menu 2-6
    - Pre-Provisioning Menu 2-7
    - Security Menu 2-8
    - Reports Menu 2-8
    - Tools Menu 2-9
    - Help Menu 2-9
  - Quick Menu Bar 2-10
  - Topology Tree 2-11
    - Organizing Network Elements in the Topology Tree 2-13
    - Moving Network Elements in the Topology Tree 2-14
    - Adding New Node Images 2-14
  - Alarm Summary 2-14
  - Main Display Window 2-15

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Viewing Tabular Data 2-15
Sorting Tabular Data 2-15
Filtering Tabular Data 2-16
Using the Online Help System 2-18
Searching for Network Elements 2-18
Configuring RMS User Preferences 2-18
Configuring the User Interface 2-18
Configuring Audible Alarms 2-19
Configuring Auxiliary Servers 2-20
Adding FTP Servers 2-20
Adding TFTP Servers 2-21
Adding Messaging Servers 2-21

CHAPTER 3 **Working with User Accounts**

Overview 3-1
Working with User Roles 3-1
Creating a New User Role 3-2
Creating the User Role 3-2
Defining User Role Privileges 3-2
Creating a User Role from an Existing Role 3-3
Viewing a User Role 3-3
Modifying a User Role 3-4
Deleting a User Role 3-4
Working with Security Policies 3-4
Creating a New Security Policy 3-5
Viewing and Modifying a Security Policy 3-7
Deleting a Security Policy 3-8
Working with User Accounts 3-8
Creating New User Accounts 3-8
Configuring a User Account for the Provisioning Server 3-10
Creating a User Account from an Existing Account 3-10
Locking and Unlocking User Accounts 3-10
Unlocking the Admin Account 3-11
Viewing and Modifying a User Account 3-12
Deleting a User Account 3-13
Resetting a User Account Password 3-13
Modifying a User Account's Security Policy 3-13
Working with a Radius AAA Server 3-14
Exporting Accounts 3-14
Creating RMS Accounts on the RADIUS AAA Server 3-14
Changing a Passphrase 3-15

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Importing User Accounts 3-15
Managing User Login Sessions 3-16
Concurrent User Sessions 3-16
Closing User Sessions 3-16
Monitoring User Activity 3-17

APPENDIX 4 **Working with Reported Data in Microsoft Excel 4-1**
Overview 4-1
Sorting RMS Report Data 4-1
Sorting Standard Alphanumeric Data 4-1
Sorting Dates and Times 4-3
Sorting by a Partial Value in a Column 4-3
Filtering RMS Report Data 4-3
Filtering Dates and Times 4-4
Filtering for Values Greater Than/Less Than a Specific Value 4-5
Clearing a Filter 4-5
Graphing RMS Report Data 4-5
Modifying Your Charts 4-6

INDEX

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

1

About This Guide

Overview

The Redline Management Suite (RMS) is a sophisticated element management solution that provides broadband network operators the ability to deploy, control, monitor and upgrade their Redline components network-wide using an intuitive user-friendly graphical interface. The Redline Management Suite acts as a gateway between your Redline equipment and your OSS/BSS, enabling full automation within your network.

RMS is a high performance, scalable Java-based application implemented using a MySQL database. Multiple operators at separate locations can use a secure, Web-based interface to access and manage broadband wireless access (BWA) network devices.

The RMS collects and stores statistical information about the managed wireless equipment. The inventory, statistical, and event information stored in the MySQL database is available to external management platforms to facilitate service provisioning, inventory, and maintenance functions through a CORBA-based northbound interface (NBI).

About This Document

This document provides an overview of the Redline Management Suite's features and how to use these features.

This document is intended for network administrators and system operators. It covers the standard operation of RMS and its optional features.

Note Unless indicated otherwise many procedures throughout this guide require that you are either logged into an RMS client session and have the correct user account privileges to access network equipment, perform upgrades and other inventory-related functions; or are logged in at the command line with root or administrative user privileges.

Using RMS to manage and monitor your Redline network elements requires a comprehensive understanding of data networking. You should also have extensive experience with configuration and operation of Redline's broadband, fixed, wireless

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

access products as part of a WiMAX network or backhaul infrastructure. Additional background knowledge should include computer operating systems and data networking theory.

Comprehensive operator and administrator training programs are available from Redline Communications. Please contact support@redlinecommunications.com for detailed information.

Document Conventions

The following document conventions are used throughout this guide.

Table 1-1 Document Conventions

Format	Description
Bold	Commands, titles, and keywords displayed in the RMS or the OS graphical user interface are displayed in bold.
<*Italic*> *User Guide:*	Arguments requiring an operator specified value are displayed in italics with angle brackets. Referenced Redline documents are also displayed in italics.
Ellipsis ...	An ellipsis before or after example text indicates there is more content either before or after the examples that are displayed. The entire contents of the file are not displayed.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Required alternative command options are grouped in braces and separated by vertical bars.
[x | y | z]	Optional command options are grouped in square brackets and separated by vertical bars.
Navigation Steps >	Successive navigational steps are indicated with an arrow. You will need to progress through the navigational path using your mouse or keyboard shortcuts.
Ctrl+click	Hold down the Ctrl key and click on line items, to select multiple items in tables or drop-down menus.

The following naming conventions are used to denote customer-specific information.

Table 1-2 Document Conventions for Customer-Specific Information

Name	Description
<*rms_host*>	Name or IP address of the host machine, on which RMS is installed.
<rms_install_dir>	Directory that contains RMS.
<*root password*>	Password for the Solaris root account.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

System Behavior

This section provides important RMS operational guidelines.

RMS Operations

- When system objects (e.g., topology tree nodes) are added or deleted, RMS may require up to 30 seconds before changes become visible to other active users.
- Passwords must contain at least one alphabetic character (e.g., A-Z, a-z). RMS will not accept passwords comprised of only numbers.
- FTP server definitions can not be deleted while they are referenced by a backup or upgrade schedule. All schedules, referencing a particular FTP server must be deleted, including schedules that have already been completed.
- The Heap size cannot exceed 1.5 GB in Windows Server 2003 OS. Refer to the *Redline Management Suite Administration and Maintenance Guide* for detailed information.
- When viewing a scheduled discovery job, all networks are displayed, even when RMS is configured for discovery of only one network. Use the check boxes to indicate which networks are to be discovered by the selected task.
- When generating reports, you can create and then generate one report at a time. You must wait for the report to complete before creating and generating another report.
- A new license file must be obtained when the licence expires (Eval only), adding new options, or updating the number of supported network elements.

Network Elements

General

- When modifying a subscriber unit wireless configuration, RMS may update and reboot the subscriber immediately, without requesting confirmation.
- When viewing information for network elements that are in the 'disconnected' state, the displayed values represent the last reported value from the network device.
- The scheduling wizards (e.g., upgrades, reports, etc.) do not support concurrent editing by multiple system users. Users attempting to modify a schedule that is currently being edited by another user will see an '**Object not found**' error and the current Web session will be terminated.
- SNMP trap destinations can not be added to Network Elements in the 'disconnected' state. The following error message is displayed: “**Unexpected Error has occurred!”** You can only add SNMP trap destinations when the network element is connected.

RedMAX

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

- Subscribers are not automatically un-provisioned when de-registered. This function must be enabled by the operator when using the nomadic feature of auto-provisioning (UnprovisionOnDeregistration setting in ProvServerConfiguration.xml). Refer to the *Redline Management Suite User Guide* for details on configuring pre-provisioned profiles. Refer to the *Redline Management Suite Installation Guide* or the *Redline Management Suite Administration and Maintenance Guide* for details on editing the RMS configuration files.
- RMS does not support reading/modifying RedMAX AN100U/AN100UX base station transmit policy parameters. You must use the AN100U CLI or a third-party SNMP tool.
- All RedMAX subscriber units to be discovered and managed by RMS, must be configured for remote management (managedSS = 1). Refer to the RedMAX documentation for details.

BWI

- When adding a new role, the RMS may display provisioning options for network elements that are not included in the current license file for that host. Unlicensed network elements are disregarded during the Discovery process.
- Software upgrades are not supported for AN80i PTP releases prior to 3.00 (FTP support was not available on these devices).
- The Mozilla FireFox™ Web browser is not supported for AN30e and the AN50e devices. You must login to RMS using Internet Explorer® and then use the RMS Pass-Through feature.

Web Client

- The Web browser cache should be cleared on all clients following any RMS upgrade.
- Always use the RMS **Refresh** button to update the RMS display. Avoid using the browser's Refresh feature.
- If the Web browser displays an error screen (e.g., 404 or java error), Close the browser and launch a new browser session. Do not use the browser's **Back** button.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Redline communications

2

RMS User Interface

Overview

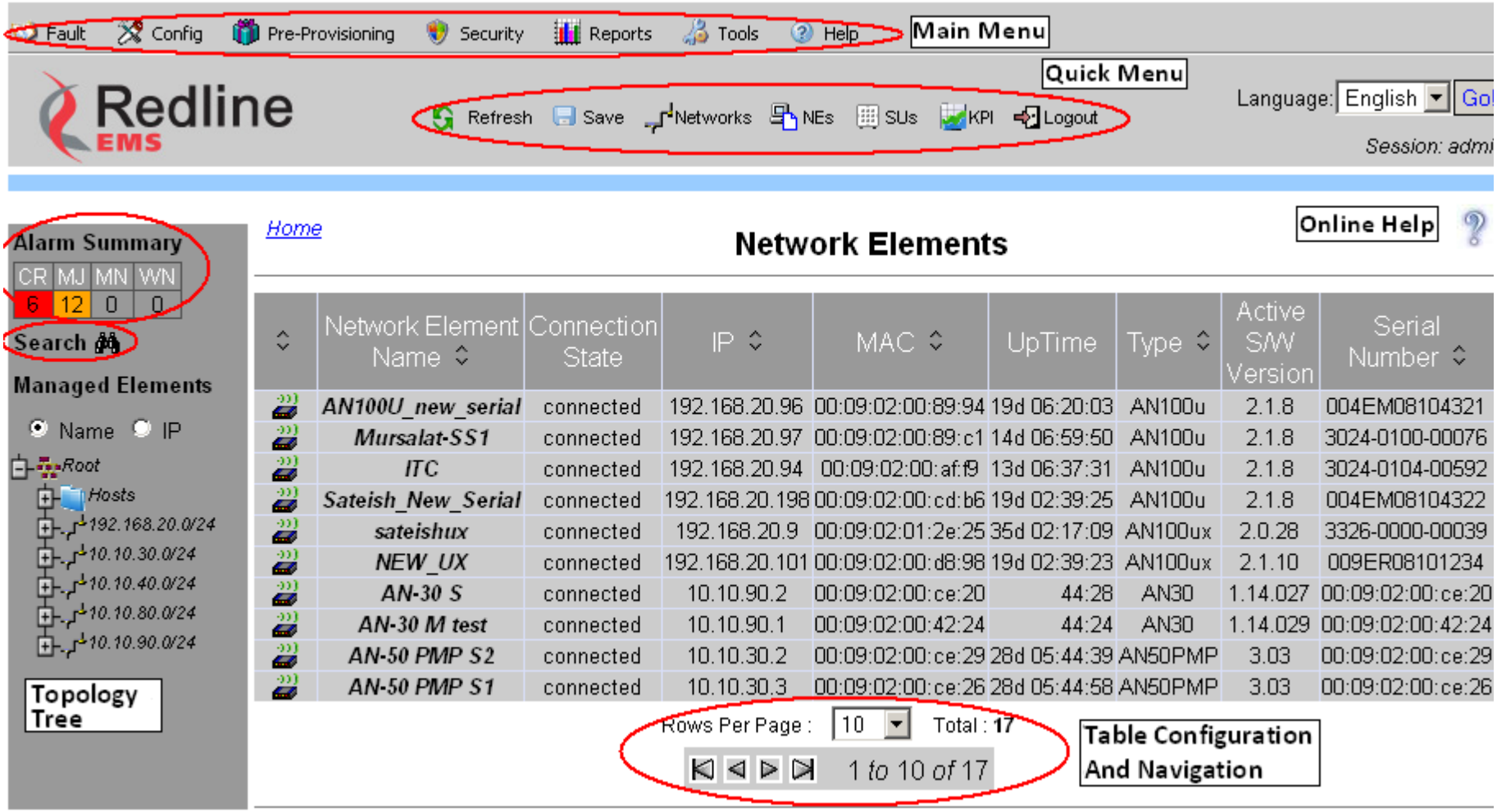
The RMS interface is web-based client GUI.

The main page consists

- Up to seven drop-down menus provide access to the many RMS features, with menu items grouped to provide access to common features. Some menus or menu items will be visible only if the associated feature has been purchased for that system.
- A Topology Tree provides an hierarchical view of your network. You can perform many of the same operations that are available from the main menu, by selecting specific sub-networks or specific devices and right-clicking to see a pop-up menu of available operations. The topology tree may be replaced by a filtering window or a wizard progress window, depending on the operations being performed in the Content Window.
- The Quick Menu bar on the RMS home page provides easy access to commonly used commands.
- The Content Window displays the results of queries and to configure various RMS operations. Control buttons are typically displayed in the lower, right corner of the window.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Figure 2-1 RMS Home Page



4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Logging into the RMS Client

While the RMS application must be installed and operated on a dedicated server, you can access the RMS client interface using an HTTP-based web browser. You must also have the Java Virtual Machine (JVM), installed on the client machine.

Each user must have a login account and may be assigned access rights based on the tasks performed by that user within RMS.

After an initial installation a user account is created with UID=admin, with PW=admin. The administrator must login and create user profiles and then create user accounts and then assign profiles to each account. Details of working with user accounts is covered in “Working with User Accounts” on page 3-8.

If you have enabled RMS to work with a RADIUS AAA server, this admin/admin account must also exist on the RADIUS AAA server. RMS will validate the UID/PW combination and if the UID can be authenticated, will then grant access to the system.

Step 1 Open your browser.

Step 2 Clear the browser cache. Refer to the online help, provided with your browser, to find out how to clear the cache.

Step 3 Enter the URL provide on the last screen of your installation.

`http://<Host_Machine_IP_Address>:8080/RedMAXEMS`

Where: The IP address is that of the RMS host machine, the RMS master host machine or the virtual IP address of the RMS high availability system.

8080 is the HTTP port. The default value is 8080, however this port corresponds to whatever port number you specified during installation.

RedMAXEMS is the name of the service.

Step 4 Enter “admin” as the user name.

Step 5 Enter “admin” as the password and then click the **Submit** button.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

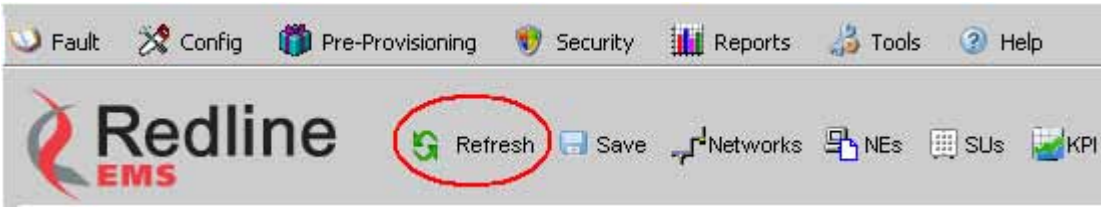
Figure 2-2 RMS Login Page

If the login is successful, the main RMS screen is displayed, as shown in Figure 2-1.

Note the following when using the RMS client in your browser:

- If the Web browser displays an error screen (i.e., 404 or java error), do not try to recover the session by clicking the browser **Back** button. Shut down the Web browser and launch a new Web browser session.
- Always use the RMS refresh button to update the RMS display and avoid using the browser refresh function.

Figure 2-3 RMS Refresh Button



4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

User Account Management

The admin/admin account is created during installation and should be used for the initial login. Once you have logged in you should change the password for this account, for security purposes. Refer to the Chapter 3 for information on managing user accounts.

Your Browser's Pop-up Blocker

If you are using the performance management and reporting option, then you must disable the 'pop-up blocker' feature in your Web browser.

If the pop-up blocker is enabled, the reports will not be displayed. Alternatively, you can use a keyboard shortcut (e.g., in Internet Explorer, hold down CTRL key) to bypass the pop-up blocker when generating a report. Refer to the online help, provided with your browser, to find out how to disable the pop-up blocker.

Working with the RMS User Interface

The RMS home page has been designed to provide easy access to all of the RMS features.

You can work through the main menu, when configuring the RMS and general network tasks such as configuring and generating reports, configuring and running maintenance tasks, etc.

You can work through the topology tree when you are working with a single network elements or you can group NE's together and apply configuration changes to the group of NEs.

Main Menu

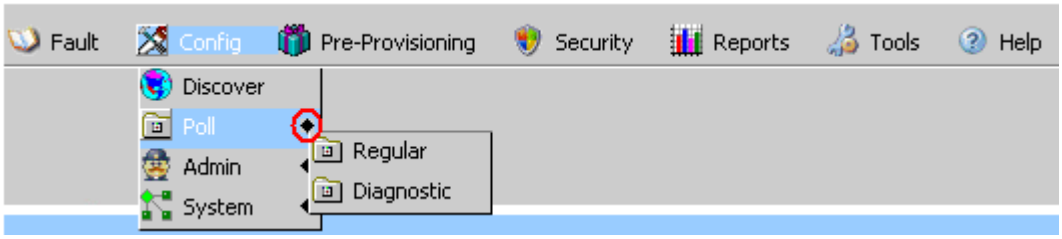
Use the main menu items for convenient access to RMS database-related functions including user management and pre-provisioning service flows.

Step 1 Move your pointer (hover) over the main menu to view the menu options. Some menu items have a further options as indicated with a black diamond at the end of the word. See Figure 2-4.

Step 2 Left-click a menu item to select it.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Figure 2-4 RMS Main Menu



A graphical representation of the RMS main menu options is provided in the *Redline Management Suite Quick Reference Guide*.

Fault Menu

Through the Fault menu, you can review and configure the RMS fault management features.

You can review current alarms, clear alarms and configure alarm notifications. Additionally you can view RMS log files, to learn more about alarm conditions.

Table 2-1 Fault Menu Options

Main Menu	Sub-Menu	Description
Alarms		Displays system alarm messages, for all devices.
Alarms History		Display, acknowledge, and clear system alarm messages.
Logs		Displays system log messages for network events, upgrades, discovery, provisioning, backups, and tasks.
Config	Alarm Severity Colors	Displays the existing colour-assignments for each alarm severity. You can change colour assignments and add sounds to alarm notifications.
	Trap Listeners	Displays the existing SNMP trap listener settings. You can modify the trap listener settings from this page.
	Alarm Severity Assignment	Displays existing SNMP traps and allows you to assign an alarm severity, alarm type, probable cause, and additional text for each alarm type.
	Alarm Notifications	Displays the rules for automatic alarm notifications. You can also modify and create new rule sets including methods to notify end users of alarm conditions (e.g., email).

Config Menu

You will configure RMS operation through the Config menu. You can configure network element discovery, device polling and auxiliary servers through this menu.

You can enable and monitor your high availability system as well as monitor the host system resources using the System option on this menu.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-2 Config Menu Options

Main Menu	Sub-Menu	Description
Discover		Displays discovered network elements and allows you to configure and execute network element discovery.
Poll	Regular	Displays the regular polling interval settings. You can enable/disable polling from this page.
	Diagnostic	Displays network elements available for diagnostic polling and allows you to enable polling by adding NEs to the list.
Admin	Scheduled Upgrades	Manage scheduled software upgrades for network elements on this page. You can also monitor the status of upgrades, that are in progress, from this page.
	Upgrades History	Display completed NE software upgrades.
	FTP Server	Display currently connected FTP servers and allows you add new servers and modify existing FTP server settings.
	TFTP Server	Display currently connected TFTP servers and allows you add new servers and modify existing TFTP server settings. This option is only displayed if you have a Provisioning Server installed.
	Tasks	Displays existing system maintenance tasks. You can create modify and scheduled existing tasks and create new tasks from this page.
	Messaging Servers	Add, delete, modify (SMTP) messaging servers.
System	Host Resources	Displays the available resources on the RMS host machine.
	System Properties	Displays RMS services and server on which they are running.
	Queues	Displays RMS system queues and their status.
	HA	Allows you to enable and monitor the status of a high availability system. This option is only displayed if your system is configured for high availability operation.
Sites		Displays information on the physical location of your sector controllers.

Pre-Provisioning Menu

You will configure profiles for new subscribers using the options on the Pre-Provisioning menu. When a Provisioning Server is included in your RMS installation, these profiles allow new users to be configured automatically, once they enter the Redline network.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-3 Pre-Provisioning Menu Options

Main Menu	Sub-Menu	Description
Service Class Bundle		Displays existing service classes and service class bundles. You can create service classes and bundles from this page.
Service Flow Bundle		Displays existing service flow bundles. You can also create service flow bundles from this page.
Network Elements		Displays existing network configuration templates. You can modify and create new templates from this page.
Subscriber		Displays a list of pre-provisioned subscriber profiles. This option is only displayed if you have a Provisioning Server installed.

Security Menu

The security menu allows you to define user roles and manage user accounts. Additionally, and you can configure the interface between RMS and AAA servers.

Table 2-4 Security Menu Options

Main Menu	Sub-Menu	Description
User Accounts		Displays a list of existing user accounts. You can create and modify user accounts from this page.
Change Password		Allows you to change the password for the current user. This option may not always be available and will depend on the user role and permissions allocated to your user account.
Change Radius Passphrase		Allows you to change the RADIUS passphrase for the current user. This option may not always be available and will depend on whether or not a RADIUS server has been configured for use with RMS and the user role and permissions allocated to your user account.
Sessions		Displays a list of users currently logged onto the RMS server, including remote hosts.
Audit Trail		Displays a log of user activity.
Roles		Displays a list of existing user roles. You can create and modify user roles from this page.
Policies		Displays a list of existing security policies.

Reports Menu

The reports menu provides access to the optional performance management features.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-5 Reports Menu Options

Main Menu	Sub-Menu	Description
Performance	Standard	Allows you to configure and create standard performance reports.
	Custom	Allows you to configure and create custom performance reports.
	Diagnostic	Allows you to configure and create diagnostic performance reports.
Events		Allows you to configure and create event reports.
System		Allows you to configure and create Provisioning Server performance reports.
Inventory		Allows you to configure and create inventory reports.
MyReports		Displays a list of all your generated reports.

Tools Menu

Provides two utilities to aid network troubleshooting. You can also configure the RMS user interface using the User Preferences option on this menu.

Table 2-6 Tools Menu Options

Main Menu	Sub-Menu	Description
Host Reachable		Allows you to verify whether or not a host device is reachable from the RMS server.
Trace Route		Allows you to perform a network trace route to a network element or other network devices (e.g., DHCP server).
User Preferences		Allows you to configure the RMS user interface

Help Menu

The Help menu provides access to the online help system as well as provides information about the RMS application.

Table 2-7 Tools Menu Options

Main Menu	Sub-Menu	Description
Support		This link takes you to the Redline Web site.
Help Contents		Displays the RMS online help system.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-7 Tools Menu Options (continued)

Main Menu	Sub-Menu	Description
About		Provides RMS version and license information.
Licences		Displays the status of the licenses for RMS and any options you have installed. Replacing or reloading the licence file is covered in the *Redline Management Suite Administration and Maintenance Guide*

Quick Menu Bar

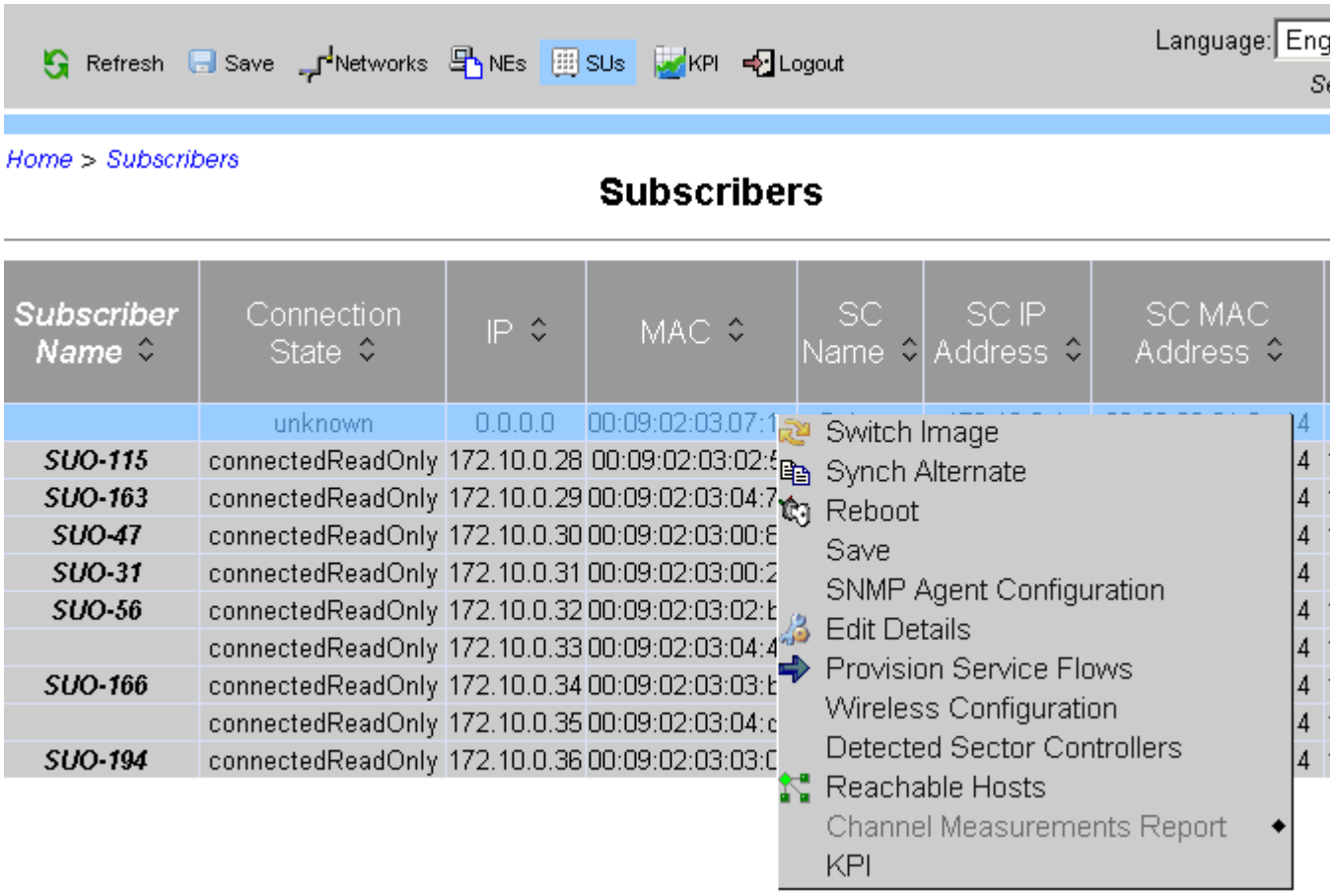
A number of frequently used operations are provided on the Quick Menu bar, as shown in Figure 2-1.The following buttons are provided:

Table 2-8 Quick Menu Operations

Button	Description
Refresh	Refresh the RMS display. Use the RMS **Refresh** button to update the RMS display and avoid using the browser refresh function.
Save	Save the NE configuration of all network elements displayed on the **Network Elements** page. The NE configuration is saved to the device's own flash memory.
Networks	List of the contents of your discovered networks as well as subscriber connection details including network device counts and a summary of network health.
NEs	List discovered sector controllers. You can select a network element from the list and right-click to access a number of commands to view and configure the selected device. The exact number of available options depends on the select device type.
SUs	List discovered subscriber units. You can filter the list using the filtering options on the left side of the **Subscribers** page. You can select a subscriber from the list and right-click to access a number of commands to view and configure the selected subscriber unit. The exact number of available options depends on the select device type. See Figure 2-5
KPI	List discovered sector controllers, for which key performance indicators are being collected. Right-click on any one of the displayed rows to see the key performance indicators for the selected device.
Logout	Logout of RMS.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Figure 2-5 RMS Quick Menu - SU button



Topology Tree

The RMS topology tree contains nodes representing discovered networks and sector controllers, and user-created logical nodes.

After network elements are discovered in a specified network, RMS automatically populates the RMS topology tree with:

- Discovered networks
- RedMAX sector controllers
- RedCONNEX and RedACCESS sector controllers and corresponding RedCONNEX/RedACCESS subscribers, located below the associated sector controller.

Each discovered subnet is displayed as a tree node, labeled with the base subnet IP address. Each discovered network element within that subnet is represented by a node labeled with the name or IP address of that element.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

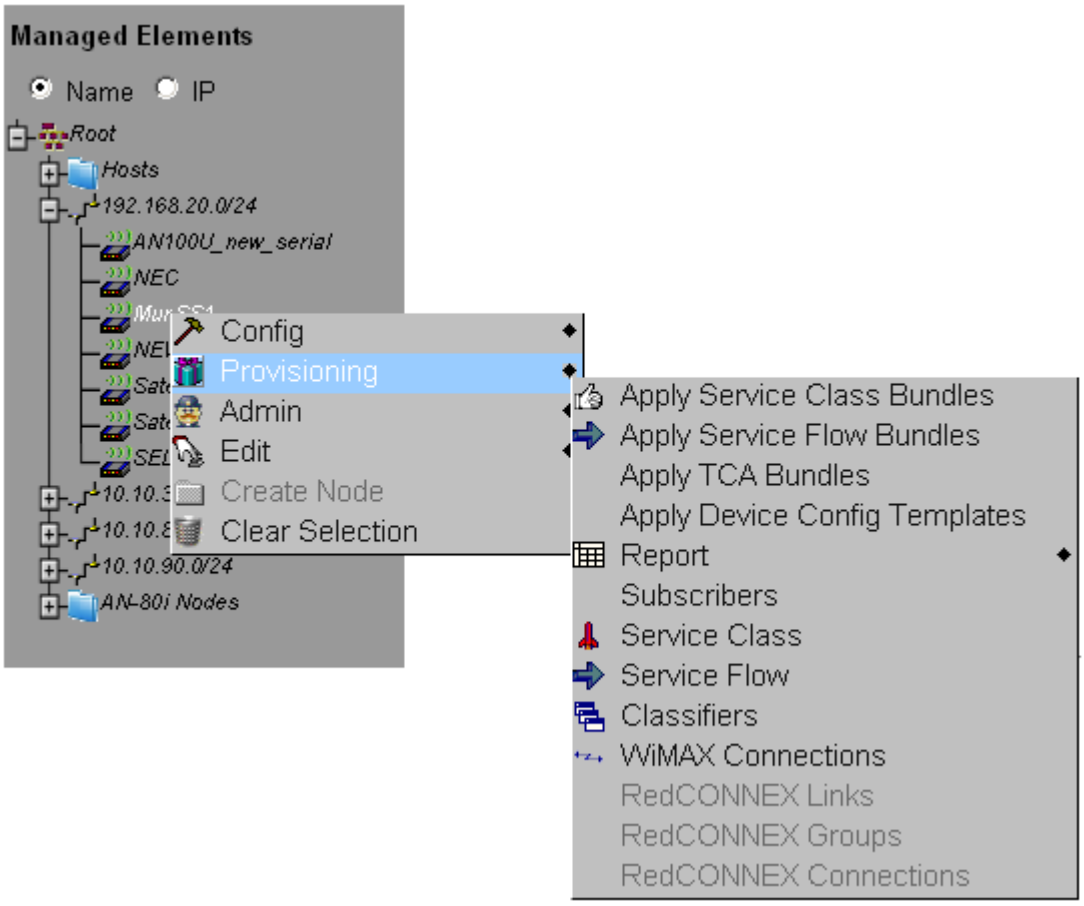
Two types of labels are used for discovered network elements: Name or IP address. You can toggle between the two views by selecting the corresponding radio button.

You can expand or collapse the grouping of network elements by clicking the icons. If required, you can create 'logical' nodes to group network elements from different subnets that are related by user applications.

You can perform a number of operations on selected nodes or on an entire network

Step 1 Select the node or network in the topology tree and right-click on it. A list of available operations pops up. As with the main menu, options indicated with a black diamond at the end of the word, have additional options that will be displayed, if selected. See Figure 2-6.

Figure 2-6 RMS Topology Tree



4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Step 2 Select the required option to display the corresponding configuration page.

Note Operations that are not available for the selected devices are greyed-out.

All operations that are available from the topology tree are listed in the *Redline Management Suite Quick Reference Guide*.

Organizing Network Elements in the Topology Tree

You can better organize your network elements, by creating hierarchies of nodes in the topology tree. You can rearrange discovered network elements, placing them in logical groups.

For example, you may want to create 'sector controller' nodes to group related sector controllers together, or place RedMAX and RedCONNEX networks below distinct and separate nodes.

Note Due to possible browser performance implications, try to keep the maximum number of logical child nodes under a parent to less than 20.

A logical node is a virtual group of physical devices. The logical node is created and managed from within RMS. There is no corresponding physical object in the network.

To create a logical node:

Step 1 In the topology tree, right-click the root item, then select **Create Node**. The **Create Logical Node** page is displayed.

Step 2 Specify the required information and click **Create**.

Table 2-9 Logical Node Creation Parameters

Parameters	Description
Name	Enter a name for the node
Description	Enter a description for the node.
Image	Select an image from this drop-down list that will appear next to the node in the topology tree.

The new node appears in the topology tree. You can now modify the node as required:

Step 3 In the topology tree, right-click the node and select **Edit** > **Edit Details**.

Step 4 On the **Edit Node** page, specify the node attributes as required, then click **Apply**.

You can also delete the node when it is no longer required:

Step 5 In the topology tree, right-click the node you want to delete, then select **Edit** > **Delete**.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Step 6 You will be prompted for confirmation. Click **Confirm** to remove the node from the topology tree.

Moving Network Elements in the Topology Tree

In RMS, you can move discovered network elements and manually-created logical nodes from one location to another. For example, for better logical organization, you can create a 'base station' folder and nest related sector controllers beneath it.

Step 1 In the topology tree, right-click on the network element or node you want to move, then select **Edit** > **Cut** (to move the node) or **Edit** > **Copy** (to create a copy of the node).

Step 2 Right-click the node under which you want the node or network element to appear, then select **Edit** > **Paste**. The node or network element appears in the new location.

Ensure network elements remain within their sub-network. If you intend to move devices between sub-networks, you will need to modify the sector controller configuration and then perform a re-discovery.

Adding New Node Images

RMS is supplied with a set of images to use when creating logical nodes in the topology tree. Additional images can be added to this library.

Note This procedure requires administrator access to the RMS file system.

Step 1 Create or acquire new images for your topology nodes. The images must be exactly 16x16 pixels. The file format must be .PNG or .GIF.

Step 2 Save new images in the following directory:

`<rms_install_dir>\images\networking`

Alarm Summary

Most RMS pages include a summary of all current alarm conditions, with counters for each severity. The Alarm Summary table is located above the topology tree on the left side of the page. See Figure 2-1.

You can configure the severity of each type of alarm. In general the following applies

- Critical (CR)—A network element event that impacts the integrity of the network
- Major (MJ)—A network element event that may cause a service interruption.
- Minor (MN)—A network element event that will not result in loss of service or data integrity, but should be corrected.
- Warning (WN)—A network element event that deviated from the expected value.

Each alarm is assigned an editable color code and wave file for audible alerts.You can modify these options through the **Alarm Severity Colors** option on the **Fault** menu.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Main Display Window

The main display window is updated as you select different options in either the main menu, or the topology tree.

Typically a table of returned results is displayed or configuration pages that allow you to configure some feature of RMS.

You can sort and filter tabular information to better suit your requirements. You can also customize the number of rows that are returned and how you navigate through all of the returned data.

Available operations are provided a buttons on the bottom of the page. These buttons will also change so that they are only applicable to the displayed data.

Viewing Tabular Data

When you are viewing tabular data, you can configure the number of rows that are displayed in each table. The number of rows that can be displayed will depend on your display settings.

Below each table you will see the number of rows displayed per page out of the total number of rows of returned data. You can navigate through the pages incrementally or you can jump to the end and then back. In Figure 2-7, ten rows of data will be displayed at a time, out of a total of 24 returned rows. You can reset the number of rows displayed on the page by clicking the drop down arrow and selecting a new value for the number of **Rows per Page.** The values that appear in this drop down box are configured under **User Preferences**, on the **Tools** menu.

Clicking on the forward button (>) will load rows 11-20. Clicking on the “end of list” (>|) button will load the rows 21-24.

Figure 2-7 Viewing Tabular Data

Sorting Tabular Data

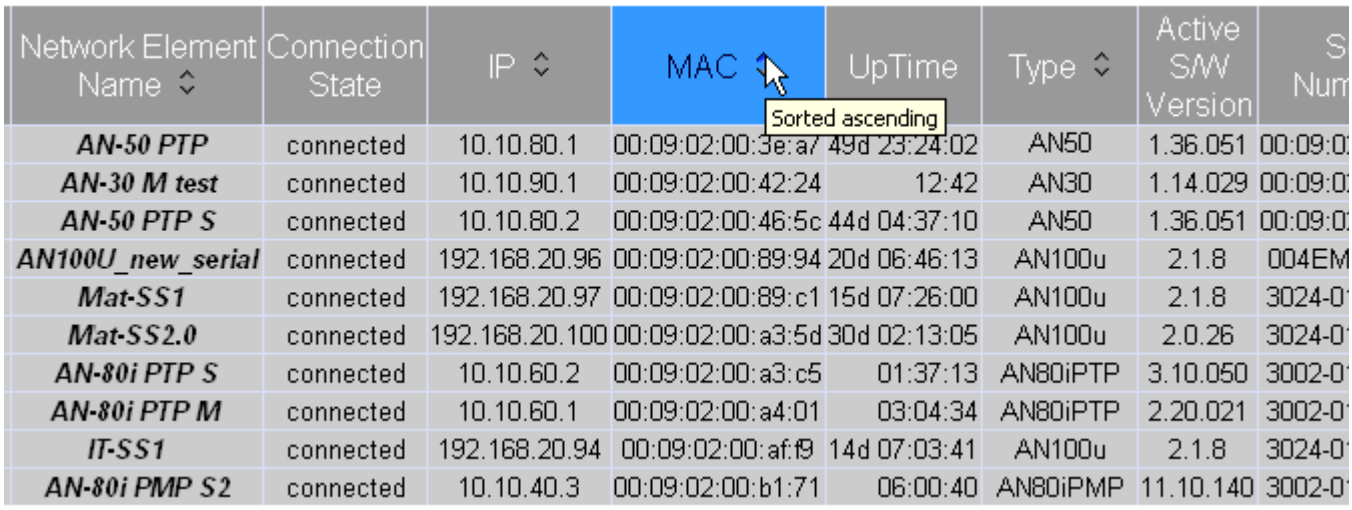
Most columns in an RMS table allow you to sort the table, based on the content of the selected column.

You can sort the displayed data using any one of the columns to define the sort order.

Double-click on the up arrow to perform an ascending sort or on the lower arrow to perform a descending sort. If you hover over the column header, a popup will tell if and how the data is sorted.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Figure 2-8 Sorting Tabular Data



Filtering Tabular Data

You can also filter tabular data. The filtering option, when available is located in the pane located on the left side of the page. Not all tabular data can be filtered.

The filtering page will be customized for the displayed data so that you can filter on specific columns. For example if you were filtering discovery log files, you could filter the list to display only the information related to your upgrade.

The filtering criteria are displayed in the pane located on the left side of the page, either directly within that pane or a tab on the pane.

Step 1 For Log files, select the **Filter** tab, on the left pane.

Step 2 The **Filter** page provides options for filtering the displayed logs according to time period, user, and discovery ID. Enter filter criteria to obtain the desired listing.

Table 2-10 Filtering Options for Discovery Logs

Parameters	Description
Time Period	Select this check box to enable filtering based on a selected time period.
Start	If you have enabled the Time period option, you need to enter the start date of the filter period. Select the Date and then Hour, Minute, and Second values for the start of the period.
Now	Select this check box to indicate the current date and time as the end of the period.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

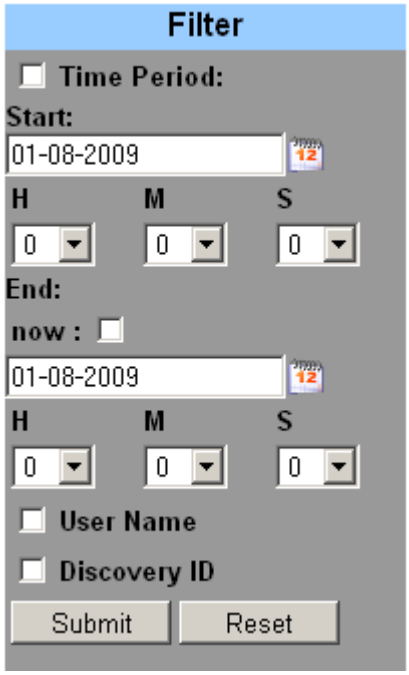
Table 2-10 Filtering Options for Discovery Logs (continued)

Parameters	Description
End	If you have enabled the Time period option, you need to enter the end date of the filter period. Select the Date and then Hour, Minute, and Second values for the start of the period.
Additional Filtering Criteria	Additional filtering criteria, specific to the displayed data are also provided. For Discovery logs these criteria would be: • User Name - Select this check box to filter log messages by RMS user account name. When selected, you will be prompted to enter the user name. • Discovery ID - Select this check box to filter log messages by the system-assigned, unique discovery ID, if known, in order to display the specific events associated with a discovery session.

Step 3 Click the **Submit** button to display log entries according to the specified filter options.

Step 4 The filtered table of results is displayed. You can sort the displayed data using any one of the columns to define the sort order. Click on the up arrow to perform an ascending sort or on the down arrow to perform a descending sort. If you hover over the column header, a popup will tell if and how the data is sorted.

Figure 2-9 Filtering Tabular Data



4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Using the Online Help System

The RMS contains an HTML-based online help system. Detailed information on each RMS page is provided by clicking on the online help button. See Figure 2-1.

The online help is context-sensitive and provides relevant information and configuration details for the specific page you are viewing. The help is displayed on a separate browser tab, so you can continue to work in the RMS client.

To display the complete Table of Contents, click on the Show TOC hyperlink at the top of any help page. This opens a new browser window with the Table of Contents, as well as Index, Search, and Glossary tabs.

You can also access the Table of Contents by clicking on the **Help** menu on the main menu.

Searching for Network Elements

Use the search feature, located above the topology to search for a network element. See Figure 2-1.

Step 1 Click on Search or the binoculars icon at the upper left of the screen.

Step 2 Enter the name or the IP address and network address mask of the missing NE. For example, enter the name ‘alpha’ or the IP address ’192.168.20.97’.

Step 3 Click **Search** to begin the search. The search results are displayed in main display page.

Step 4 Click **Cancel** to stop the search and hide the search dialog box.

Configuring RMS User Preferences

You can configure various aspects of the GUI and Alarm notifications. Each user can configure their GUI and the changes they make to their account are saved in the database and available each time they log into RMS.

Configuring the User Interface

Step 1 Click on the **Tools** Menu and select **User Preferences**.

Step 2 There are three tabs on the **User Preference** tab. Select the **UI** tab.

You can configure the following information on this tab.

Table 2-11 User Interface Customization Options

Parameters	Default Value	Description
Table		
Ordinary Refresh Rate	30 seconds	Controls the rate at which standard tables (such as the Network Elements table) are refreshed.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-11 User Interface Customization Options (continued)

Parameters	Default Value	Description
Results Refresh Rate	10 seconds	Controls the rate at which results tables (such as the results page shown after applying a service flow bundle) are refreshed.
Rows per Page Option		Controls the options for the default number of rows per table that are displayed in the drop down box, below each table. See Figure 2-7.
Rows per Page	10 Rows	Controls the default number of rows per table that are displayed on each page. You can click the **Validate** button, to verify the settings are valid.
Topology Tree		
Managed element Labels		Controls the displayed labels of managed devices in the topology tree. You can choose to display the assigned element name or the element's IP address.
Queues		
Threshold for Current Queued Tasks		Specify a threshold value for queued tasks. This value is used to highlight queues in **Queues** page that exceed this threshold.

Step 3 Enter your preferences and click **Submit.**

Step 4 You can click the **Defaults** button to restore the default values for all parameters on this page.

Configuring Audible Alarms

Step 1 Click on the **Tools** Menu and select **User Preferences**.

Step 2 There are three tabs on the **User Preference** tab. Select the **Alarms** tab.

You can configure the following information on this tab.

Table 2-12 User Interface Settings

Parameters	Default Value	Description
Alarm Table		
Refresh Rate	10 seconds	Controls the rate at which the Alarms table is refreshed.
Audible Alerts		

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-12 User Interface Settings (continued)

Parameters	Default Value	Description
Critical	Critical01.wav Enabled	By default, audible alerts are enabled. To disable audible alerts for any alarm, select Disabled in the corresponding drop-down list. For each alarm severity, a corresponding sound file is selected by default. Use this dialog to change the selection for any alarm type. Custom alert sounds can be added to RMS. In order for the custom sound to be available on this page, you must first save the .WAV file to the following directory on the RMS host machine: <rms_install_dir>\web\webapps\RedMAXEMS\repository \audio All .WAV files in this directory can be selected from these drop-down lists.
Major	Major01.wav Enabled	
Minor	Minor01.wav Enabled	
Warning	Warning01.way Disabled	

Step 3 Enter your preferences and click **Submit.**

Step 4 You can click the **Defaults** button to restore the default values for all parameters on this page.

Configuring Auxiliary Servers

After installation you will need to configure supporting applications to utilize all of the RMS features. You will need to configure FTP or TFTP servers for upgrading and backing up network element configuration. You will require a messaging server to send alarm messages or to send reports.

Adding FTP Servers

FTP and TFTP servers are required during network element configuration backup/restore and software upgrade operations. Saving information on existing FTP and TFTP servers in the RMS database allows you to select known FTP or TFTP servers instead of having to specify them during these operations.

Step 1 Navigate to the **Config** > **Admin** > **FTP Server**. The **FTP Servers** page is displayed.

Step 2 Click **Add** to add a new server. The **Add/Modify FTP Server** page is displayed.

Step 3 Specify the required details of the FTP server.

Step 4 Click **Add** to store the FTP server configuration in the RMS database.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-13 FTP Server Configuration Parameters

Parameter	Description
FTP User Name	Specify the user name for this FTP server.
FTP Password	Specify the password for this FTP user. Retype the FTP password in the following row to confirm the password.
FTP Address	Specify the IP address of this FTP server.
Max Number of NEs	Specify the maximum number of NE configurations that can be stored on this FTP server. This number is capped at 10000 network elements. Note In order to support 10000 network elements, your FTP server host machine must have significant memory resources.

Adding TFTP Servers

Step 1 Navigate to the **Config** > **Admin** > **TFTP Server**. The **TFTP Servers** page is displayed.

Step 2 Click **Add** to add a new server. The **Provision TFTP Server** page is displayed.

Step 3 Specify the required details of the TFTP server.

Table 2-14 FTP Server Configuration Parameters

Parameter	Description
Server Address	Specify the IP address of this TFTP server.
Server Port	Specify the TFTP server port number; usually 69.
Server Folder	Specify the full path to the 'base' directory of the TFTP server.
Server Description	Specify a brief description of the TFTP server (optional).

Step 4 Click **Provision** to store the FTP server configuration in the RMS database.

Adding Messaging Servers

You must configure an SMTP server in order for RMS to email reports and automatic alarm notifications.

Step 1 Navigate to the **Config** > **Admin** > **Messaging Server**. The **Messaging Servers** page is displayed.

Step 2 Click **Add** to add a new server. The **Add Messaging Server** page is displayed.

Step 3 Specify the required details of the messaging server.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 2-15 FTP Server Configuration Parameters

Parameter	Description
Server Name	Specify the name for this messaging server.
Server Address	Specify the IP address of this TFTP server.
Server Port	Specify the TFTP server port number; usually 69.
Server Folder	Specify the full path to the 'base' directory of the TFTP server.
Server Description	Specify a brief description of the TFTP server (optional).

Step 4 Click **Provision** to store the FTP server configuration in the RMS database.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

3

Working with User Accounts

Overview

The Redline Management Suite supports multiple client users. RMS allows you define various levels of user access, define security policies and then finally create user accounts using the roles, and polices which ensures the user accounts are consistent and reduces both account management and security issues.

You will first create user roles that define system access and thus the user's job. The RMS system allows you to create new user roles with the ability to match your users' abilities with their responsibilities. Next you will create both password and user policies that define the access to the RMS system. RMS does not permit access without authentication. Additionally, all management activity is reflected in an activity audit trail. Once roles, and polices have been created, you can easily create user accounts.

RMS allows the administrator to manage client users individually and at the group level through user roles. Individual user accounts can be locked, modified, duplicated, deleted, and the password can be reset. You can modify system access at the user role level.

You can also authenticate users through a RADIUS AAA server. When you install RMS you will need to enable and configure this feature. Refer to the *Redline Management Suite Installation Guide* for detailed instructions. If you are using a RADIUS AAA server, user accounts must be created on the RADIUS AAA server first and then created in RMS. If you are adding a RADIUS AAA server to your existing installation, you will need to export existing RMS accounts and then create these accounts on the RADIUS AAA server.

Working with User Roles

The following default roles are defined in RMS:

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 3-1 Default User Roles

Role	Description
Admin	This role is associated with the default administrative account. The admin user has full read/write and execute rights to all RMS resources.
Operator	This role is associated with the default operator account. The operator has full read/write and execute rights to all RMS resources except security management, such as creating users, granting access permissions, etc.
Monitor	This role is associated with the default network monitoring account. The monitor has read-only access to all RMS resources.

Creating a New User Role

You can create new user roles to better suit your business processes. In order to create new roles, you must be logged in as an administrator and have full access to the system.

When creating new user roles, you want to provide each user with only the access that they need to perform their jobs. If users are performing more than one task, they can be assigned to multiple user roles.

Creating the User Role

To create new user roles:

Step 1 Navigate to **Security** > **Roles**.

Step 2 Click on the **Add** button. In the **Add Roles** page, enter a name and a description for the new role. The name must be at least 5 characters long.

Defining User Role Privileges

You will now define the user role's privileges. The column on the left side of the Roles page shows the RMS resources. These resources are shown in a tree-structure. Clicking on the top branch will display the available options. As you open each branch, a description of the operation is shown in the second column. You can click on the online help button ( ) to see information on each of the options.

By default, the user role is denied read/write access to all resources. You will only need to select the resources required for your new role.

You can enable read/write access to all resources, by selecting the top branch of the tree: **Resources**. In general, only one administrator will have full access. You do not want other user roles to have full system access for security purposes.

You can enable read/write access to all resources belonging to any given branch, by selecting that branch. For example, if you navigate down to **Fault**, de-select the **Deny** checkbox and enable the **Read** checkbox, you will enable read access to all Fault resources.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

If you enable write access, read access is added automatically. To define your user role's privileges:

Step 1 De-select the **Deny** checkbox. You can now select Read and/or Write access for the selected resource.

Step 2 Click on the **Read** and/or **Write** checkbox beside each resource that you want for your user role.

Step 3 Click the **Add** button.

Step 4 Your new role will be created and will appear in the list of user roles, along with the creation date.

When you are creating user roles, RMS may display access to RedACCESS or RedCONNEX network elements that are not included in your license file. RMS will not be able to establish connectivity with these devices, even if they are discovered in your network.

Ensure that these devices are not included in your user roles unless your RMS licence file included these devices. Contact support@redlinecommunications.com for information on how to update your RMS licence file.

Creating a User Role from an Existing Role

You can also create a user role, using an existing role as a template.

Note You cannot duplicate the user role, if the user role is currently in use. i.e. a user is logged in with the selected role assigned to his/her user account.

Step 1 Navigate to **Security** > **Roles**.

Step 2 Select the user role to be used as the template and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Duplicate** option.

Step 4 In the **Add Roles** page, enter a name and a description for your new role.

Step 5 Define your user role's privileges. De-select the **Deny** checkbox and select Read and/or Write access for the selected resources.

Step 6 Click the **Add** button to create the user role.

Viewing a User Role

Once a user role has been created you can view the accessible resources.

Step 1 Navigate to **Security** > **Roles**.

Step 2 Select the user role and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **View** option.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Step 4 In the **Role's Details** page, you can open branches and view the resources to which the selected role has read/write access.

Modifying a User Role

You modify a user role to change the user's privileges.

Note You cannot modify the user role, if the user role is currently in use. i.e. a user is logged in with the selected role assigned to his/her user account.

Step 1 Navigate to **Security** > **Roles**.

Step 2 Select the user role and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Modify** option.

Step 4 In the **Modify Role** page, you can open branches and modify the read/write access to the resources.

Step 5 Click the **Save** button to save your changes to the RMS database.

Deleting a User Role

You can delete a user role that is no longer in use.

Note You cannot delete the user role, if the user role is currently in use. i.e. a user is logged in with the selected role assigned to his/her user account.

Step 1 Navigate to **Security** > **Sessions** and ensure that there are no users, with the user role to be deleted, currently logged onto RMS.

Step 2 Navigate to **Security** > **Roles**.

Step 3 Select the user role and then right-click on the row.

Step 4 From the drop-down menu that is displayed, select the **Delete** option.

Step 5 You will be prompted to confirm the deletion of the selected user role. Click the **Confirm** button if you really want to delete the displayed user role.

The role will be deleted and it no longer appears on the **Roles** Screen.

Working with Security Policies

User accounts are defined with a User Policy and a Password Policy. With these policies, the administrator can create a variety of standard policies and reference them individually to customize user accounts. Each policy can be created or modified through the GUI.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

A User Policy governs the rules for managing the age of an account and its associated password, the maximum number of concurrent sessions per user, the maximum number of failed login attempts, and the length of RMS session for that user account.

A Password Policy governs the rules for enforcing password format specifics, such as minimum/maximum length, whether to require the inclusion of numeric characters, or whether to allow a user name to be part of a password.

Creating a New Security Policy

Step 1 Navigate to **Security** > **Policies**.

Step 2 The **Security Policy** page is displayed.

Step 3 Click on the **Add** button to create a new policy. In the **Add Policy** page, select the type of policy you are creating.

Step 4 The **Add Policy** page is updated to display the specific details for your new policy.

Step 5 Enter the details of the password policy as outlined in the following table.

Table 3-2 Password Policy Parameters

Parameter	Description
Policy Type	You can create a password policy or a user policy. The parameters on the screen will be updated to match the policy type you have selected.
Policy Name	Enter a name for your new policy.
Minimum Length	Enter a minimum length for your password. Passwords with too few characters are easier to resolve. A password with a minimum of 8-characters is recommended. The default value is 5 characters.
Maximum Length	Enter a maximum length for your password. If users are entering lengthy passwords and are then unable to remember them, you may need to reduce the maximum password length. The default value is 40 characters.
Enforce Numeric Characters	Enable this check box if you want the passwords to contain numbers as well as alphabetic characters.
Allow User Name to be in Password	Enable this check box if you want to allow the user to enter their user name as the password or as part of the password.

Alternatively, enter the details of the user policy as outlined in the following table then click the **Save** button to create the new policy.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 3-3 User Policy Parameters

Parameter	Default	Description
Policy Type	N/A	You can create a password policy or a user policy. The parameters on the page will be updated to match the policy type you have selected.
Policy Name	N/A	Enter a name for your new policy.
Password Warning Age	0 days	Enter the number of days after which you want to warn the user to change their password. The default value of zero days means no warning is ever displayed.
Password Locking Age	30 days	The number of days (age) after which the account will be locked. A value of zero days means the password age does not result in account locking.
Password Deletion Age	0 days	The number of days (age) after which the account will be deleted. The default value of zero days means password age does not result in account deletion.
Account Warning Age	0 days	Enter the number of days after which you want to warn the user that their temporary account is about to expire. The default value of 0 days means there is no warning. If you have set an **Account Deletion Age** or an **Account Locking** Age, you should set reasonable **Account Warning Age**.
Account Deletion Age	0 days	Enter the number of days after which you want to delete a temporary user account.
Account Locking Age	0 days	Enter the number of days after which you want to lock a temporary user account. A value of zero indicates that the account will never be locked. Account Locking Age, is designed for temporary users and is intended for accounts that are active for less than one year. The account age is measured by subtracting the current date from the account creation date. If the account is more than one year old, then you will not be able to unlock the account even by setting the maximum account age to 365 days. If the account status is **Account Locking Age has expired**, then you need to set the **Account Deletion Age** parameter to 0 and manually unlock the account. See “Unlocking the Admin Account” on page 3-11.
Number Of Unique Consecutive Passwords	8 Passwords	Enter the number of unique passwords that your users must use before re-using the same password. The default value is 8 passwords. This means that, when prompted to change their password, the user must enter a password that is different from the past 8 passwords that have been used. A value of zero means the user can re-enter the same password indefinitely.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 3-3 User Policy Parameters (continued)

Parameter	Default	Description
Maximum Number Of Concurrent Session Per User	8 Sessions	Enter the number of sessions that a user can create, concurrently.
Maximum Number Of Login Before Password Change	0 Logins	Enter the maximum number of successful login attempts before the user must change their password. A value of zero means the password will never expire. A password that does not expire poses a significant security risk.
Maximum Number Of Failed Login	3 Attempts	Enter the maximum number of failed login attempts before the user account is locked. You will then need to manually unlock the account. See “Unlocking the Admin Account” on page 3-11.
Session Timeout	30 Minutes	Enter the number of minutes of inactivity, after which the user session times out and is closed. After the session times out, the user must login again. Any tasks that were running will continue to run to completion. Any session-specific client queries will be stopped. Note Do not set the Session Timeout to 0 (zero). If you exit the browser without first logging off you will eventually cause a lockout condition due to the high number of abandoned, active sessions.

Viewing and Modifying a Security Policy

You can modify security policies at any time. Changes that you make to policies that are associated with accounts will impact those users. You need to advise users of impending changes to their accounts.

Note You will also need to carefully consider the impact of your potential policy changes on the admin user account. It may be best to create user and password policies that are used only for the admin account.

Step 1 Navigate to **Security** > **Policies**.

Step 2 Select the policy that you want to modify and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Modify** or **Details** option.

Step 4 If you selected the Modify option, the **Modify Policy** <*name*> page is displayed. Update the required parameters. Click the **Save** button to apply the changes.

Step 5 If you selected Details, you can view the current settings for the selected policy.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Deleting a Security Policy

You can delete a security policies at any time. Changes that you make to policies that are associated with accounts will impact those users. You must advise these users of impending changes to their accounts.

Step 1 Navigate to **Security** > **Policies**.

Step 2 Select the policy that you want to delete and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Delete** option.

Step 4 You will be prompted to confirm the deletion of the selected policy. Click the **Confirm** button if you really want to delete the displayed policy. The policy will be deleted.

Working with User Accounts

Once you have defined the user roles for your application, you can begin creating user accounts. When creating user accounts, you may want to limit the number of accounts that you create for both security and performance considerations.

Creating New User Accounts

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 The **New User Account** page is displayed. You will need to enter the user information, as outlined in Table 3-4, below.

Step 3 Once you have entered the data, click on the **Add** button to create the user. If you have entered all of the required information correctly, the user account will be created. If information is missing, you will be returned to the **New User Account** page where missing information will be indicated in red.

Table 3-4 Entry Fields for Creating New User Account

Field Name	Description
User Name	Enter the account user's name. The account name must be alphanumeric. It must be at least 5-characters long. Do not use spaces or restricted characters. In order to avoid conflicts with the operating system and the database, do not use the following characters in user names or passwords: / \ *, : ; = +? | < > & % ' **"**. If you have a defined user account naming policy, please refer to your system administrator for details of the account naming conventions.
Password	Enter the password for authenticating this user. The password must be a minimum of 5 characters and adhere to the password policy, if specified.
Confirm Password	Enter the account user's password again, for verification.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 3-4 Entry Fields for Creating New User Account (continued)

Field Name	Description
Description	Enter a description of the user account. For example, if this account will be used to provision new subscribers, you may want to indicate that information here.
Password Policy	Select a password policy from the list. If you have created password policies, they should be displayed here. If you need to create a policy, see “Creating a New Security Policy” on page 3-5. If no policy is required, select **Default**.
Roles	Select one or more user roles to define the access that this user account will have to the RMS resources. You can select more than one user role, by holding down the Ctrl-key while clicking on the desired user roles.
User Policy	Select a user policy from the list. If you have created user policies, they should be displayed here. If you need to create a policy, see “Creating a New Security Policy” on page 3-5 If no policy is required, select **Default**.
Email Configuration	
Recipient	Check this box, if you want to enable this account to receive email messages. Once this option is enabled, you will need to specify the address and provide a description.
E-Mail Address	Specify the recipient's full email address. i.e. tech@network.com Since only the sender will actually send emails through the configured SMTP server, recipients only need their address added to the “To” list so that the mail server can find them.
User Description	Specify a description of the recipient or the recipient’s display name.
Sender	Check this box, if you want to enable this account to send email messages. In order to use this feature your SMTP server information must already exist in the RMS database. Once this option is enabled, you will need to specify details of the SMTP server.
E-Mail Address	Specify the sender’s full email address or SMTP account name, depending on the authentication requirements of the SMTP server.
User Description	Specify a description of the sender or the sender’s display name.
Password	Enter the sender’s password for the associated SMTP account.
Confirm Password	Enter the sender’s password, again for verification.
Server	Select the SMTP server from which incoming mail can be retrieved.
Default Sender	Check this box, if you want RMS to use the selected SMTP account for all outgoing mail.
admin	This field specifies the user as an Admin user.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Configuring a User Account for the Provisioning Server

When you are using the Provisioning Server, you need to create a unique user account that will be used by the Provisioning Server to login to the NBI and communicate with RMS. Refer to the *Redline Management Suite Installation Guide* for detailed instructions on configuring the account for the Provisioning Server.

You should also create a separate user account for any other NBI clients to facilitate traceability and troubleshooting. Refer to the *Redline Management Suite Administration and Maintenance Guide* for details on referencing the user account from the NBI application.

Creating a User Account from an Existing Account

You can also create a user account, using an existing one as a template.

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Select the user account to be used as the template and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Duplicate** option.

Step 4 In the **Duplicate Users** page, enter a new name and password. The remaining account information can remain the same.

Step 5 Click the **Save** button to create the user account.

Locking and Unlocking User Accounts

You can lock accounts to prevent users from accessing the RMS server. Only the Administrative user, with appropriate access can lock and unlock user accounts.

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Select the user account that you want to lock and then right-click on the row. Use Ctrl+click to select multiple rows.

Step 3 From the drop-down menu that is displayed, select the **Lock** option.

Step 4 In the **Lock** page, enter a reason for locking the account and click **OK**.

Step 5 The account will now be locked. The user account is now inaccessible and the user cannot login to the RMS Server. If the user attempts to login they will see a message indicating that the user account is locked.

To unlock the account:

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Select the user account that you want to unlock and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Unlock** option. The account will be unlocked.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Unlocking the Admin Account

Each user will be allowed to attempt to log into the RMS server a number of times. The exact number of retry attempts is determined by the associated security policy.

If for some reason you have entered the incorrect login information a number of times and become locked out of the system, there is now no way to unlock the account from the GUI.

You can unlock the administrative account from the command line, using the userAccUtil utility reset the lock. In general you should use the GUI to manage user accounts. The userAccUtil utility should only be used when there are no GUI methods to manage an account. The userAccUtil utility allows you to unlock an account as well as display information about a specific account or all user accounts.

The userAccUtil utility has the following usage:

`userAccUtil unlock <username> | display <username> | display_all | display_locked_accts`

There are two additional commands, only available to the administrative/root user:

userAccUtil reset_password <*privileged username*> <*privileged password*> <*userNameForWhichToResetPassword*> <*newPassword*> | reset_radius_password <*privileged username*> <*privileged password*> <*newRADIUSPassword*> | reset_locking_age <*privileged username*> <*privileged password*> <*userNameForWhichToResetLockingAge*> <*newLockingAge*>

Where	username	This is the RMS user name.
	privileged username	This is the user ID of the system administrative/root user, root
	privileged password	This is the password of the system administrative/root user.
	userNameForWhichToResetPassword	This is the RMS user name, for which you want to reset the password.
	newLockingAge	This is the duration for which the new password will be in effect. The user will be prompted to change the password at the end of the locking age.
	newPassword	This is the new password for the specified user.
	newRADIUSPassword	This is the new RADIUS password for the associated RADIUS Server. This password is used to authenticate the communication between RMS and the Radius server

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Windows Server 2003

Step 1 As the administrative user, navigate to the command line interface on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 Navigate to the bin directory, within the installation directory:

```
cd <rms_install_dir>\bin
```

Step 3 Run the utility, specifying the operation and the account user name:

```
userAcctUtil.bat unlock admin
```

Solaris 10

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<password>
```

Step 2 Navigate to the following directory, within the installation directory:

```
cd <rms_install_dir>\bin
```

Step 3 Run the utility, specifying the operation and the account user name:

```
userAcctUtil.sh unlock admin
```

Viewing and Modifying a User Account

Once a user account has been created you can view the settings at any time.

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Select the user account and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **View** option.

In the **User Account's Details** page, you can see the current settings. To modify the account use the following procedure:

Step 1 Navigate to **Security** > **Roles**.

Step 2 Select the user account and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Modify** option.

Step 4 In the **Modify User** page, you can modify any of the user account settings.

Step 5 Click the **Save** button to save your changes to the RMS database.

Note Changing a user role assignments (or access level) will result in the user being logged-off to allow for your changes to take effect.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Deleting a User Account

You can delete a user account that is no longer is use. Before deleting the account, ensure the user is not logged into the system.

Step 1 Navigate to **Security** > **Sessions** and ensure the user is not currently logged onto RMS.

Step 2 Navigate to **Security** > **User Accounts**.

Step 3 Select the user account and then right-click on the row. Use Ctrl+click to select multiple rows.

Step 4 From the drop-down menu that is displayed, select the **Delete** option.

Step 5 You will be prompted to confirm the deletion of the selected user account. Click the **Confirm** button if you really want to delete the displayed user account.

Step 6 The account will be deleted and no longer appears on the **User Accounts** page.

Resetting a User Account Password

If a user has forgotten their password or you want to transfer a user account to a new user, you can reset the password.

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Select the user account and then right-click on the row.

Step 3 From the drop-down menu that is displayed, select the **Reset Password** option.

Step 4 You will be prompted to confirm this action for the selected user account. Click the **Confirm** button if you really want to reset the password.

Step 5 Enter the new password and then enter it again for verification.

Step 6 Click the **Save** button to change the password.

Modifying a User Account's Security Policy

You can modify one or both of the security policies applied to a user account. You can modify the policies for a single account using the Modify action. You can modify the policies for one or more accounts using the Apply Policy action.

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Select the user account and then right-click on the row. Use Ctrl+click to select multiple rows.

Step 3 From the drop-down menu that is displayed, select the **Apply Policy** option.

Step 4 On the **Apply Policy** page, select the new User Policy and/or the new Password Policy for the selected account.

Step 5 Click the **Apply** button to apply the selected policies to the selected accounts.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Working with a Radius AAA Server

If you configured RMS as a RADIUS client during installation then RMS is now the client and sends user login requests to the RADIUS AAA server. The RADIUS AAA server receives the RMS user request for access, attempts to authenticate the user, and returns configuration information and applicable polices to RMS, if the user has been authenticated. If the user cannot be verified the access request is refused.

Exporting Accounts

If you are adding a RADIUS AAA server to your existing RMS installation. You will need to add all of the users that you have created for RMS to the RADIUS AAA server. To facilitate the addition of user information on you can export a list of users from RMS.

Depending on the size and level of activity in your network, you may have many RADIUS AAA servers to which requests will be forwarded, to increase performance. This is load balancing. You must configure RMS to take advantage of load balancing, during installation. Additionally, you must add your RMS users to each of the RADIUS AAA servers that will be used to load balance client requests.

The export file will be in XML format and you can use this data to create the users on the RADIUS AAA server.

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Click the **Export Users** button to export existing RMS account information to the following file:

`cd <rms_install_dir>\conf\<RMSUser_`*`date_time`*`>.xml`

The date and time, at which the file was created, is appended to the file name so that you can perform multiple exports without overwriting the file.

Note You require the schema file, RMSUsers.xsd to view and interpret the export file correctly.

Refer to the documentation provided with your RADIUS AAA server for detailed instructions on creating users on the RADIUS AAA server. General guidelines are provided in the *Redline Management Suite Installation Guide*.

Creating RMS Accounts on the RADIUS AAA Server

Detailed instructions for adding users are provided with your specific version of the RADIUS server. In general you need to add all of the RMS users and their passwords to your RADIUS server. This may be in the form of a text file or may require entering information into the database configured for the server. Consult your system administrator for detailed information

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

You will also need to verify the password shared between RMS and the RADIUS server. The password and the type of authentication (PAP or CHAP will have been configured during installation.

Changing a Passphrase

If the passphrase has been changed on the RADIUS AAA server then you need to change the passphrase for your RMS user account as well.

Do not change this passphrase, unless the passphrase has already been changed on the RADIUS AAA server.

Step 1 Navigate to **Security** > **Change Passphrase**.

Step 2 On the **Change Passphrase** page, enter the new password and then enter it again for verification. Enter the previous passphrase.

Step 3 Click the **Save** button to change the passphrase.

Step 4 In a separate browser window, log into RMS again to verify the passphrase was changed correctly.

Importing User Accounts

If RMS is being installed in a network where a RADIUS AAA server is already managing accounts you will need to import the existing, authenticated users and then apply a RMS user role, user and password policy to each account.

RMS will import files in XML format as defined by RMSUsers.xsd. The RMS Users XML schema definition file is located in the following directory:

`<rms_install_dir>\conf\RMSUsers.xsd`

Step 1 Navigate to **Security** > **User Accounts**.

Step 2 Click the **Import Users** button. The **Import Users** page is displayed.

Step 3 Use the tree view of your RMS installation directory to select the location of the import file. Click on the file to select it and click **Load**. The imported users appear at the bottom of the page.

Step 4 Select the user accounts to be added to RMS. Use Ctrl+click to select multiple rows.

Step 5 Select the user role, the password policy and the user policy to apply to each user account, that has been selected. The incoming user names and passwords must comply with the selected password policy and the user policy.

Step 6 Click **Add**. The selected rows will be removed from the table and be added as RMS user accounts.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

If you see an error message, indicating that the passwords do not comply with the existing RMS policy, you will need to create a new RMS policy to accommodate the RADIUS AAA server passwords.

Step 7 To verify the operation, navigate to **Security** > **User Accounts**.

The imported users will now be listed on the **User Account** page. The description will indicate that these user accounts have been imported. The applied user role, password policy and user policy can be changed at any time after the user is imported into RMS.

If you do make any changes to a user's password, password policy or user policy, within RMS, then you must export the user files and update the user account information on the RADIUS AAA server(s).

Note You can export user accounts without using the RADIUS server.

Managing User Login Sessions

Concurrent User Sessions

A session is the time during which a user is logged on and is working on the RMS server. You can have a maximum number of 25 concurrent users. The maximum number of users will be determined by what users are doing on the system and your system resources

Each of those users can also have a number of concurrent sessions, as defined by their user policy. There is also a maximum number of sessions allowed per client and ultimately per RMS server.

If a user exceeds the number of allowed, concurrent sessions, they need to close some of their open sessions, by logging out.

Alternatively, you can increase the number of allowed concurrent sessions. This setting will take effect when you click on the Add/Save button.

Closing User Sessions

You can close user sessions, as required, to address performance issues or if the session becomes unusable for any reason.

Step 1 Navigate to **Security** > **Sessions**.

Step 2 The following information is displayed for each session:

Table 3-5 Session Parameters

Parameter	Description
User Name	User account associated with this session.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 3-5 Session Parameters (continued)

Role(s)	Roles associated with this user account.
Session Id	Unique identifier for this user session.
Login Time	Date and time of user login for this session.
Idle Time	Indicates the time this session has been idle (for automatic logoff).
Session Type	Indicates the mode used for this session: Web Session: User is logged in through HTML browser. Console Session: User is logged in through EMS console
Remote Address	Network IP address of RMS user, if known.

Step 1 Select the session that you want to terminate and then right-click on the row.

Step 2 From the drop-down menu that is displayed, select the **Terminate** option.

Step 3 You will be prompted to confirm the action. Click the **Confirm** button if you really want to terminate the session.

Monitoring User Activity

You can monitor user activity within a session using the Audit trail feature.

Step 1 Navigate to **Security > Audit Trail**.

Step 2 The **View Audit Trail Log** page is displayed and shows all user activity for RMS from the time the application was installed. You can filter the list to display only the information related to a specific user, session ID, or date range.

Step 3 In the pane located on the left side of the page, enter your required options for filtering the displayed user information according to time period, user, and session ID.

Table 3-6 Filtering Options for Audit Logs

Parameters	Description
Time Period	Select this check box to enable filtering based on a selected time period.
Start	If you have enabled the Time period option, you need to enter the start date of the filter period. Select the Date and then Hour, Minute, and Second values for the start of the period.
Now	Select this check box to indicate the current date and time as the end of the period.
End	If you have enabled the Time period option, you need to enter the end date of the filter period. Select the Date and then Hour, Minute, and Second values for the start of the period.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table 3-6 Filtering Options for Audit Logs (continued)

Parameters	Description
User(s)	Select this check box to filter messages by the RMS user account. When selected, you will be prompted to select the user account name from the drop-down list. You can select multiple users using Ctrl+click.
Session ID	Select this check box to filter information by the system-assigned, session ID, to display the specific events associated with a single login session.

Step 4 Click the **Submit** button to display log entries according to the specified filter options. You can click the **Reset** button to reset the filter and display all log entries.

Step 5 When the filtered table of results is displayed, you can further sort the displayed data using any one of the columns to define the sort order. Click on the up arrow to perform an ascending sort or on the lower arrow to perform a descending sort. If you hover over the column header, a popup will indicate if and how the data is sorted. See “Sorting Tabular Data” on page 2-15.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Redline communications

4

Working with Reported Data in Microsoft Excel

Overview

Once you have generated your report data, as outlined in Chapter 6, and the reports have been saved to Microsoft® Excel™ format (.XLS), you have many options to work with the data.

The data can be further sorted and filtered and you can generate many different type of charts.

The following procedures are specific to Microsoft Excel 2007 and will vary slightly depending on the version of Excel that you are using. In addition to Microsoft Excel, you can use almost any spreadsheet application, that imports .XLS files, to work with the RMS reports. Additionally, you can use this data in any Microsoft Office application such as Word or PowerPoint.

Sorting RMS Report Data

You can sort your RMS report data using the extensive sorting options provided by Microsoft Excel. Before working with your data in Excel, you may want to make backup copies of the reports or split reports containing data for multiple network elements.

Sorting Standard Alphanumeric Data

You can sort data by text (A to Z or Z to A), numbers (smallest to largest or largest to smallest), and dates and times (oldest to newest and newest to oldest) in one or more columns. You can also sort by a custom list (such as Large, Medium, and Small).

Sort criteria are saved with the workbook/worksheet so that you can reapply your sort each time you open the workbook/worksheet for an Excel table, but not for a range of cells. If you want to save sort criteria so that you can periodically reapply a sort when you open a workbook, then it's a good idea to use a table. This is especially important for multi-column sorts or for sorts that take a long time to create.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Step 1 Open your report in Excel.

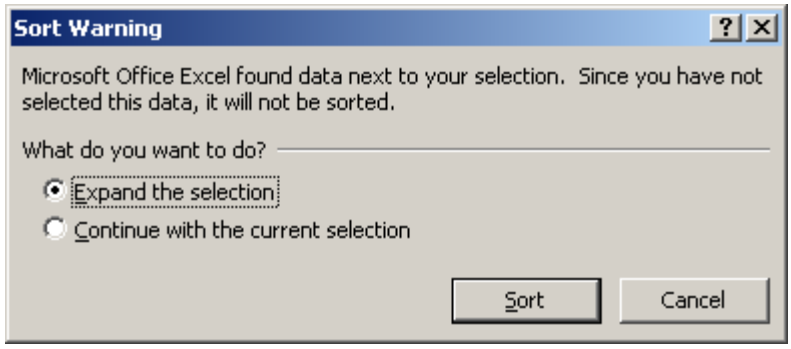
Step 2 Select a cell or a range of cells in a table column, on which you want to sort the data.

Step 3 On the **Data** tab, in the **Sort & Filter** group, do one of the following:

- To sort in ascending alphanumeric order, click **Sort A to Z**.
- To sort in descending alphanumeric order, click **Sort Z to A**.

Step 4 The table data will be sorted as you have selected. If you selected a range of cells within the column, you will be prompted to extend the selection to include the other columns in the table. You must select **Expand the Selection**.

Excel will display the following message:


Sort Warning
Microsoft Office Excel found data next to your selection. Since you have not selected this data, it will not be sorted.
What do you want to do?
Expand the selection
Continue with the current selection
Sort
Cancel

Note You must select **Expand the Selection**. If you do not select this option, only the selected column will be sorted and your report data will then be invalid. Sorting by one column in a range will produce results that you don't want.

If the data is not sorted as you expect, verify the data as follows:

- Ensure that all data is stored as text. If the column that you want to sort contains numbers stored as numbers and numbers stored as text, then you need to format your data as text. If you do not, the numbers stored as numbers are sorted before the numbers stored as text. To format all of the selected data as text, on the **Home** tab, in the **Font** group, click the **Format Cell Font** button, click the **Number** tab, and then under **Category**, click **Text**.
- Remove any leading spaces. In some cases, data imported from another application might have leading spaces inserted before data. Remove the leading spaces before sorting the data.
- If a cell is empty, this cell is treated as a regular excel missing values and not a value of zero or an empty string. Excel handles empty strings differently from missing values.
- In order to ensure that you sort by number values, move your mouse over first value in the range, that is to be sorted and click to select it. Do not select the column name.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Refer to the online documentation provided with Microsoft Excel to see more detailed information on creating customized sorting criteria.

Sorting Dates and Times

You can also sort data by dates and times.

Step 1 Select a single cell or a range of cells containing dates or times, on which you want to sort the data.

On the **Data** tab, in the **Sort & Filter** group, do one of the following:

- To sort from an earlier to a later date or time, click **Sort Oldest to Newest**.
- To sort from a later to an earlier date or time, click **Sort Newest to Oldest**.

Step 2 The table data will be sorted as you have selected. If you selected a range of cells within the column, you will prompted to extend the selection to include the other columns in the table. You must select **Expand the Selection**.

If the data is not sorted as you expect, verify the data as follows:

- Ensure that dates and times are stored as dates or times. In some reports a time range is stored (i.e. 13:00-14:00), in this case Excel cannot resolve this value as a time. you will need to split the value into two column or treat the data as text.

  In order for Excel to sort dates and times correctly, all dates and times in a column must be stored as a date or time serial number. If Excel cannot recognize a value as a date or time, the date or time is stored as text. You will need to convert dates stored as text to dates and/or times.

Sorting by a Partial Value in a Column

Sorting is based on the entire value in a column. If you want to sort by part of a value in a column, such as a device name (AN80i-WST-16), time range (i.e. 13:00-14:00), you first need to split the column into two or more columns so that the value you want to sort by is in its own column. To do this, you can use functions or the **Convert Text to Columns Wizard**. Refer to the online documentation provided with Microsoft Excel to see more detailed information on functions and converting a single column to multiple columns.

Filtering RMS Report Data

Filtering data is a quick way to find and work with a sub-set of data in a range of cells or in a table. Once you have filtered data in a range of cells or table, you can either save the data as a separate report, or clear a filter to display all of the data.

Filtered data displays only the rows that meet the conditions you specify to limit which records are included in a query or filter. The filtering process hides rows that you do not want displayed. After you filter data, you can copy, find, edit, format, chart, and print the subset of filtered data without rearranging or moving it.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

You can also filter by more than one column. Filters are additive, which means that each additional filter is based on the current filter and further reduces the subset of data. For example, if you are working on an inventory report and only want to see only SUO network elements with a specific software version, you would filter the list by **NE Type** and **Software Active Version.**

Note When you use the **Find** dialog box to search filtered data, only the data that is displayed is searched; data that is not displayed is not searched. To search all the data, clear all of your filters.

Step 1 Select a range of cells containing alphanumeric data.

Step 2 On the **Data** tab, in the **Sort & Filter** group, click **Filter**. A filter icon appears at the top of the selected column.

Step 3 Click the arrow in the column header. In the drop down list you will see all of the criteria, on which you can filter your data. All of the options are selected, by default. Clear **Select All** to clear all of the check boxes, and then select the specific text values to filter by. Click **OK** to filter your data.

The rows containing data that does not match your selection will be hidden, displaying only the data that does match your selection.

To determine if a filter is applied, note the icon in the column heading:

- A drop-down arrow means that filtering is enabled but not applied. When you hover over the heading of a column with filtering enabled but not applied, a screen tip displays **Showing All**.
- A **Filter** button means that a filter is applied. When you hover over the heading of a filtered column, a screen tip displays the filter applied to that column, such as **Equals SUO**.

Refer to the online documentation provided with Microsoft Excel to see more detailed information on creating customized filtering criteria.

Filtering Dates and Times

The procedure for filtering dates and times is the same as outline above, with one exception. In the filtering drop down box, all dates in the selected range of cells or table column are grouped by an hierarchy of years, months, and days. Selecting or clearing a higher level in the hierarchy selects or clears all nested dates below that level. For example, if you select 2009, months are listed below 2009, and days are listed below each month.

Again, as with sorting data, if the data is not filtered as you expect, ensure that dates and times are stored as dates or times. In order for Excel to sort dates and times correctly, all dates and times in a column must be stored as a date or time serial number. If Excel cannot recognize a value as a date or time, the date or time is stored as text. You will need to convert these values to dates and/or times.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Filtering for Values Greater Than/Less Than a Specific Value

Step 1 Select a range of cells containing numeric data.

Step 2 On the **Data** tab, in the **Sort & Filter** group, click **Filter**.

Step 3 Click the arrow in the column header. Point to **Number Filters** and then do one or more of the following:

- To filter by numbers that are greater than a specific value, click **Greater Than** or **Greater Than Or Equal To**.
- To filter by numbers that are less than a specific value, click **Less Than** or **Less Than Or Equal To**.

Step 4 Enter your specific value in the **Custom Autofilter** dialog box and click **OK** to filter your data accordingly.

There are a number of other options in the **Number Filters** menu, including the option to filter numeric values above or below the column average. Excel also provided text filters that allows you to match specific text string. Refer to the online documentation for more details.

Clearing a Filter

To clear a filter for one column in a multi-column range of cells or table, click the **Filter** button on the heading, and then click **Clear Filter** from <Column Name>.

To clear all filters in a worksheet and display all rows, on the **Data** tab, in the **Sort & Filter** group, click **Clear**.

Graphing RMS Report Data

Graphing or creating charts of your data allows you to provide a visual interpretation of your data. For most users it is easier to recognize trends or view relative performance when viewing date in a graphical format.

Depending on how your RMS reports are generated, they may already include charts. The charts that are already included in an RMS report cannot be modified through Excel. In order to modify these charts, you would have to regenerate the report directly through RMS. Charts that you create in Excel can be saved with the spreadsheet and be used to supplement the those charts generated by RMS.

A chart has many elements. Some of these elements are displayed by default, others can be added as needed. You can change the display of the chart elements by moving them to other locations on your chart, resizing them, or by changing the format. You can also remove chart elements that you do not want to display.

You start creating a chart by selecting the data for the chart from your RMS report. Typically, RMS data is arranged in columns. Depending on your selection, Excel automatically determines the best way to plot the data in the chart. Some chart types (such as pie charts) require a specific data arrangement.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Step 1 Open your RMS report in Excel. Navigate to **Reports** > **MyReports**. Select the required report and double-click on it. You may be prompted to select the target application.

Step 2 Sort or filter your RMS report data to obtain the desired data set, as outlined in the previous sections.

Step 3 Select the complete range of cells for your graph. You can select non-adjacent columns column using hold down the Ctrl-key and dragging your mouse over the columns to be included in your chart.

Step 4 On the **Insert** tab, in the **Chart** group, click on type of chart you want to create.

Step 5 Your chart will be created. Review your chart and save your spreadsheet with the chart.

Modifying Your Charts

After you create a chart, you can modify it. For example:

- You may want to change the way that axes are assigned. The y-axis is usually the vertical axis and contains data. The x-axis is usually the horizontal axis and contains categories, but can also contain data.
- To help clarify the information that appears in your chart, you can add a chart title, axis titles, and data labels.
- You can show or hide a legend or change its location. In some charts, you can also show a data table that displays the legend keys in a chart. Legend keys appear to the left of legend entries. Formatting a legend key also formats the data marker that's associated with it and the values that are presented in the chart.
- You can also apply special options for each chart type. Special lines, such as high-low lines and trendlines that provide a graphic representation of trends in a data series and other options are available for different chart types.

Refer to the Excel’s online documentation for more details.

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Index

A

Admin User Role 3-2
Alarm
  Configuring Audible 2-19
  Summary Table 2-14
Audit
  Trail Log 3-17

B

Browser
  Clearing Cache 2-3

C

Client, Launching in Browser 2-5
Config Menu
  Overview 2-6
Configuring
  Audible Alarms 2-19
  RMS User Preferences 2-18
Creating
  Security Policy 3-5
  User Account 3-8
  User Roles 3-2

D

Deleting
  Security Policy 3-8
  User Account 3-13
  User Role 3-4
Document
  Conventions 1-1
  Overview 1-1

F

Fault Menu
  Overview 2-6
Filtering
  Audit Logs 3-17
  Discovery Log Entries 2-16
  Report Data in Microsoft Excel 4-3
  RMS Tabluar Data 2-16
FTP Server
  Adding 2-20

G

Graphing
  Report Data in Microsoft Excel 4-5

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

H

Help Menu 2-9
RMS Online System 2-18

I

Importing User Accounts 3-15

L

License
Network Elements Managed by RMS 3-3
Status of Current File 2-10
Log, Audit Trail 3-17
Log Entries
Filtering 2-16

M

Managing
User Sessions 3-16
Microsoft Excel, Working with RMS Reports . 4-1
Modifying
Security Policy 3-7
User Account 3-12
User Role 3-4
Monitor User Role 3-2

N

Network Element
Included in RMS License 3-3
Organizing in Toplogy Tree 2-13
Search 2-18

O

Online Help 2-18
Operator User Role 3-2

P

Password
Applying Pollicy to Imported Accounts . . . 3-16
Resetting 3-13
Security Policy 3-4
Popup
Blocker 2-5
Pre-Provisioning
Menu Overview 2-7

Q

Quick Menu Bar 2-10

R

RADIUS AAA Server
Importing Accounts from 3-15
Reports
Filtering Data 4-3
Graphing Data 4-5
Menu Overview 2-8
Sorting Data 4-1
Working with Microsoft Excel 4-1
RMS
Launching GUI Client 2-5

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

S

Searching for Network Elements 2-18
Security Menu 2-8
Security Policy 3-4
  Creating 3-5
  Deleting 3-8
  Modifying 3-7
  Parameters 3-6
  Types 3-5
  Viewing 3-7
Session
  Managing 3-16
  Parameters 3-16
Sorting
  Audit Logs 3-17
  Report Data in Microsoft Excel 4-1
  RMS Tabular Data 2-15
Special Characters 3-8

T

TFTP Server
  Adding 2-21
Tools Menu 2-9
Topology Tree
  Organizing Network Elements 2-13
  Overview 2-11

U

User Account 3-8
  CLI Utility 3-11
  Creating 3-8
  Deleting 3-13
  Duplicating 3-10
  Importing 3-15
  Modifying 3-12
  Modifying Security Policy 3-13
  Parameters 3-8
  Resetting Password 3-13
  Restricted Characters 3-8
  Security Menu 2-8
  Unlocking Admin Account 3-11
  Viewing 3-12
User Interface
  Preferences 2-18
  RMS 2-5
User Policy
  Applying to Imported Accounts 3-16
  Security 3-4
User Preferences 2-18
User Role
  Access to Network Elements 3-3
  Applying to Imported Accounts 3-16
  Creating 3-2
  Defining Privileges 3-2
  Deleting 3-4
  Duplicating 3-3
  Modifying 3-4
  Options 3-1
  Read/Write Access 3-2
  Viewing 3-3
Utility
  userAcctUtil.bat 3-11

V

Viewing
  RMS Tabluar Data 2-15

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Security Policy 3-7
User Account 3-12
User Role 3-3

W

Working
with RMS Tables 2-15
with User Interface 2-5

4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299